Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

# ANNIHILATORS OF MODULAR INVARIANTS AND COVARIANTS.*

BY OLIVE C. HAZLETT.

## Introduction.

1. **Abstract and relation to the literature.** Up to the present, not very much has been accomplished toward developing a theory of modular covariants for the general case—i.e., for the general form or for the general field. Dickson has proved that modular invariants and covariants of any system of binary forms possess the finiteness property when the coefficients of the transformations are marks of any Galois Field $GF[p^n]$ of order $p^n$,† and fundamental sets of invariants, seminvariants and covariants have been found by various writers for the more important special cases.‡ But in these latter papers, one is struck by the fact that the methods used are ones which apply admirably to the cases considered but in some way fail of complete generality.§

Nevertheless, the results for the different special cases have analogies, some of which are rather striking. Some of these analogies are shown in the conditions that a given function $\varphi$ be a seminvariant of a form $f$ and in the closely related subject of annihilators of invariants and covariants. A few years ago, Professor Dickson || found annihilators of modular semin-

---

* Read before the American Mathematical Society, September 6, 1920. The work of this paper has been facilitated by the purchase of an abstract journal and other books from a grant made by the American Association for the Advancement of Science.

Since finishing this MS., there has appeared an article by W. L. G. Williams on "Formal modular seminvariants" (presented to the American Mathematical Society October 30, 1920; published in the Transactions of the American Mathematical Society for January, 1921), in which he proves Theorem III of the present paper. Nevertheless, I have decided to leave my own paper unchanged, especially since his proof does not seem to me very convincing (see § 6).

† "General theory of modular invariants," Trans. Amer. Math. Soc., vol. 10 (1909), pp. 123–158; "Proof of the finiteness of modular covariants," ibid., vol. 14 (1913), pp. 299–310.

‡ Dickson's results are summarized in his Madison Colloquium Lectures, "On invariants and the theory of numbers" (1914). Glenn, "A fundamental system of formal covariants modulo 2 of the binary cubic," Trans. Amer. Math. Soc., vol. 19 (1918), pp. 109–118; "Modular concomitant scales with a fundamental system of formal covariants, modulo 3, of the binary quadratic," ibid., vol. 20 (1919), pp. 154–168.

§ Perhaps this statement should be qualified. The methods of constructing invariants and covariants have generality in that they are applicable to other cases and some of them are applicable even for general modulus $p$ or for the general form $f$; but none of them is applicable to all covariants of every form.

|| Invariants of binary forms under modular transformations," Trans. Amer. Math. Soc., vol. 8 (1907), pp. 205–232.

variants of the binary quadratic and binary cubic analogous (in a general way) to those in classical invariant theory. Then he found a set of annihilators for modular seminvariants of a binary quadratic (or cubic) for some of the Galois Fields $GF[p^n]$ of order $p^n$, where $p$ is a small prime and $n$ is greater than 1. This gives at once necessary conditions that a polynomial $\varphi$ be a seminvariant of $f$. For the cases considered, he verified that these conditions are also sufficient.*

The present paper attacks the problem in a slightly different way and obtains results which apply to any system of binary forms and any Galois Field $GF[p^n]$ of order $p^n$. The annihilators of modular invariants obtained in this manner are of the type anticipated in the paper by Professor Dickson; so also are the set of necessary and sufficient conditions that a polynomial $\varphi$ be a modular seminvariant. It is interesting to note that these operators are also annihilators of formal modular invariants if no reductions are made by Galois' generalization of Fermat's Theorem ($a^{p^n} \equiv a$). Hence, since the modular covariants of a system $S$ may be obtained from the modular invariants of an enlarged system $S'$, we readily have annihilators of modular covariants. In the same manner, we obtain annihilators of formal modular covariants. These annihilators lead to a set of $n$ necessary and sufficient conditions that a polynomial $\varphi$ be a modular covariant (formal or otherwise).

2. **Summary of previous results.** The first published work on annihilators of modular invariants was in a paper by Dickson. As he there pointed out, the differential operators which annihilate an invariant are more complicated in the theory of modular invariants than in the theory of classic invariants, for in a series of powers of an arbitrary mark $t$ of the $GF[p^n]$, certain terms now combine—namely, $t^i$, $t^{i+\mu}$, $t^{i+2\mu}$, $\cdots$, where $\mu = p^n - 1$. Bearing this fact in mind, and applying Taylor's Theorem, he finds annihilators for some special cases.

For the first example, he considers the form

$$a_0x^2 + a_1xy + a_2y^2, \tag{1}$$

in which the coefficients are integers reduced modulo 3. Let $\varphi$ be a polynomial in the $a$'s with all exponents $\leq 2$. There is no loss of generality in doing this, since any polynomial may be reduced to this form by applying Fermat's Theorem, which in this case gives us $a^3 \equiv a \pmod 3$. Under the transformation

$$\begin{aligned} x &= x' + ty', \\ y &= y', \end{aligned} \tag{2}$$

let $a_1$ and $a_2$ be transformed into $a_1 + \alpha_1$ and $a_2 + \alpha_2$ respectively, and let $\varphi$ be transformed into $\varphi'$. Then, by Taylor's Theorem, $\varphi' - \varphi$ is readily expressed as a polynomial in $\alpha_1$ and $\alpha_2$, in which the exponents of the $\alpha$'s are $\leq 2$ and the coefficients are partial derivatives of $\varphi$ with respect to $a_1$ and $a_2$ divided by an integer relatively prime to 3.

---

* For an outline of his results, the reader is referred to § 2 of the present paper.

By rearranging terms, it is evident that

$$\varphi' - \varphi = t\delta_1\varphi + t^2\delta_2\varphi,$$

where $\delta_1\varphi$ and $\delta_2\varphi$ are differential operators on $\varphi$. A necessary condition that $\varphi' \equiv \varphi$ is clearly $\delta_1\varphi \equiv 0$. It is not so evident, however, that this is also sufficient. In the classical case, $\delta_2\varphi$ is readily shown to be $\frac{1}{2}\delta_1(\delta_1\varphi) = \frac{1}{2}\delta_1{}^2\varphi$. The classic procedure does not obtain here because $\delta_1$ is a differential operator which applies only to a polynomial in which the exponents are all $\leq 2$, whereas the polynomial $\delta_1\varphi$ does not have all its exponents $\leq 2$. Hence we have no right to talk about $\delta_1(\delta_1\varphi)$ in this case. If we let $[\delta_1\varphi]$ denote $\delta_1\varphi$ in reduced form, i.e., with every exponent $\leq 2$, then $\delta_1[\delta_1\varphi] \equiv \frac{1}{2}\delta_2\varphi$. Hence it follows that $\delta_1\varphi \equiv 0$ is both a necessary and sufficient condition that $\varphi' \equiv \varphi$; that is, $\varphi$ is a seminvariant of the binary quadratic modulo 3 if and only if $\delta_1\varphi \equiv 0$.

Dickson found that a similar statement can be made about the seminvariants of the other special cases that he studied, provided that the field is a Galois Field $GF[p^n]$ of order $p$ where $p$ is a prime.

But, just as soon as we consider seminvariants of a quantic in the $GF[p^n]$, where $n > 1$, then difficulties arise. If $\psi$ is a polynomial in $t$ of degree $\leq \mu = p^n - 1$, then

$$\psi(a + t) - \psi(a) = t\psi'(a) + \frac{t^2}{2!}\psi''(a) + \cdots + \frac{1}{i!}t^i\psi^{(i)}(a) + \cdots + \cdots + \frac{1}{\mu!}t^\mu\psi^{(\mu)}(a).$$

When $n > 1$, the denominators $i!$ are not all relatively prime to $p$. Consider the quantic

$$a_0x^m + a_1x^{m-1}y + a_2x^{m-2}y^2 + \cdots + a_my^m \tag{3}$$

and subject $x$ and $y$ to the transformation

$$x = x' + ty', \quad y = y'. \qquad (t \text{ in the } GF[p^n]). \tag{4}$$

If $\varphi$ is any polynomial in the $a$'s, and $\varphi'$ denotes its transform, then

$$\varphi' - \varphi \equiv t\delta_1\varphi + t^2\delta_2\varphi + \cdots + t^i\delta_i\varphi + \cdots + t^\mu\delta_\mu\varphi, \tag{5}$$

where the $\delta_i$ are differential operators. Professor Dickson considered special quantics when $n > 1$, and from his results he conjectured that in general necessary and sufficient conditions that $\varphi$ shall be an invariant of (3) under the group of transformations (4) are the vanishing of $\delta_i\varphi$ where $i = 1, p, p^2, \cdots, p^{n-1}$.

Nine years later, Professor Glenn* observed that, for the $GF[p]$, any formal covariant would have to be annihilated by

$$(6) \qquad \Upsilon = O_0 + O_1 x \frac{\partial}{\partial y} + O_2 x^2 \frac{\partial^2}{\partial y^2} + \cdots + O_j x^j \frac{\partial^j}{\partial y^j} + \cdots.$$

He does not say what the $O_j$ are except that they are partial differential operators "in the derivatives with respect to the coefficients of (3), non-homogeneous as to the derivatives the orders of which range from zero to infinity in each $O_j$." In this paper he points out that, if we proceed as in the proof of Robert's Theorem on the unique-determination of an algebraic covariant from its leader, we get relations among the coefficients of the covariant and the operators $O_j$ which are not recurrent as they are in the classic case. Under special conditions, he gives these relations; but they are so complicated that they do not seem particularly useful.

## Annihilators for $GF[p]$.

3. **A preliminary formula.** Consider a system $S$ of forms with coefficients, the $a$'s, which are marks of the Galois Field $GF[p^n]$ of order $p^n$. Let $\varphi$ be any polynomial of the $a$'s. When we subject the variables $x$ and $y$ to the transformation

$$(7) \qquad \begin{aligned} x &= x' + ty' \\ y &= y' \end{aligned} \qquad (t \text{ any mark in } GF[p^n]),$$

let the $a$'s be transformed into the $a'$'s and let $\varphi$ be transformed into $\varphi'$. Then, by the Lie theory,

$$(8) \qquad \varphi' - \varphi = t\,\Omega\varphi + \frac{t^2}{2!}\Omega^2\varphi + \cdots + \frac{t^k}{k!}\Omega^k\varphi + \cdots,$$

where

$$\Omega\varphi = \left.\frac{\partial \varphi'}{\partial t}\right|_{t=0}, \qquad \Omega^2\varphi = \Omega(\Omega\varphi) = \left.\frac{\partial^2 \varphi'}{\partial t^2}\right|_{t=0},$$

and, in general,

$$\Omega^k\varphi = \Omega(\Omega^{k-1}\varphi) = \left.\frac{\partial^k \varphi'}{\partial t^k}\right|_{t=0}.$$

Note that $\Omega$ is the Aronhold annihilator for the case when the $a$'s and $t$ are in the field of ordinary complex numbers. Hence, for the classic case, a necessary and sufficient condition that $\varphi' = \varphi$ is that $\Omega\varphi = 0$. This is not true, however, when $t$ and the $a$'s are marks of a finite field, since then the different powers of $t$ are not distinct and thus certain terms coalesce. If $t$ is any mark of the Galois Field $GF[p^n]$ of order $p^n$, then $t^{p^n} \equiv t$ in the field (by Galois' generalization of Fermat's Theorem). Thus, in the field, we have the congruence

---

* "The formal modular invariant theory of binary quantics," Trans. Amer. Math. Soc., vol. 17 (1916), pp. 545–556, especially pp. 547–548.

$$(9) \qquad \varphi' - \varphi \equiv t \sum_{k=0}^{\infty} \frac{\Omega^{1+k(p^n-1)}}{[1 + k(p^n - 1)]!} + t^2 \sum_{k=0}^{\infty} \frac{\Omega^{2+k(p^n-1)}}{[2 + k(p^n - 1)]!} + \cdots + t^{p^n-1} \sum_{k=0}^{\infty} \frac{\Omega^{(k+1)(p^n-1)}}{[(k + 1)(p^n - 1)]!} .$$

In each of these coefficients, it must be borne in mind that the division by the factorial is purely a formal one. This is legitimate even when the factorial is not relatively prime to $p$, since $\partial^q \varphi / \partial t^q$ is always exactly divisible by $q!$. We shall write (9) for convenience in the form

$$(9') \qquad \varphi' - \varphi = t\delta_1\varphi + t^2\delta_2\varphi + \cdots + t^\mu\delta_\mu\varphi,$$

where $\mu = p^n - 1$.

4. **Significance of the differential operators.** Before proceeding any further, it will be well to pause a moment to consider the full force of the operators $\delta_k$. When the $a$'s and $t$ are independent variables, then $\varphi' - \varphi$ is given by (8), where $\Omega$ is the classical Aronhold annihilator denoted by $U$ in Lie's theory. But when the $a$'s and $t$ are indeterminate marks of the $GF[p^n]$, then $\varphi'$ may be written in a variety of ways and for each such way of writing $\varphi'$ we get a different expansion for $\varphi' - \varphi$. When $\varphi'$ denotes the result of replacing the $a$'s by the $a'$'s in a purely formal manner—i.e., without reducing by the aid of Fermat's Theorem, we shall say $\varphi'$ is written in unreduced form. If we go to the extreme of reducing the exponents of the $t$ so that they are all $\leq \mu = p^n - 1$, then

$$(10) \qquad \varphi' - \varphi \equiv t \frac{\partial \varphi'}{\partial t}\bigg|_{t=0} + \frac{t^2}{2!}\frac{\partial^2 \varphi'}{\partial t^2}\bigg|_{t=0} + \cdots + \frac{t^\mu}{\mu!}\frac{\partial^\mu \varphi'}{\partial t^\mu}\bigg|_{t=0} .$$

But $\dfrac{\partial \varphi'}{\partial t}\bigg|_{t=0}$ is not now the same as $\Omega\varphi$ and the derivatives of higher order are not now the same as the corresponding iterations of $\Omega$. In fact, in the coefficients of $t$ we will now have not only the coefficient of $t$ when $\varphi'$ is written in unreduced form, but also the coefficient of $t^{1+p^n-1}$, of $t^{1+2(p^n-1)}$, etc. Hence the coefficient of $t$ in (10) is the sum of a number of expressions—viz., the partial derivatives of the unreduced $\varphi'$ with respect to $t$ of orders $1$, $1 + (p^n - 1)$, $1 + 2(p^n - 1)$, $\cdots$. A similar statement applies to the coefficients of the other powers of $t$ in (10).

But $\varphi' - \varphi$ is also given by the congruence (9). Hence, in (9), the coefficient of $t$ is actually congruent to the first partial derivative of $\varphi'$

with respect to $t$ if we reduce by Fermat's Theorem before differentiating; the coefficient of $t^2$ is congruent to $1/2!$ times the second partial derivative of $\varphi'$ with respect to $t$ if we reduce by Fermat's Theorem first; and so on. Since this is true of any polynomial $\varphi'$ in the $a$'s, then we would expect that the coefficient of $t^2$ would be found by applying the operator

$$D_1 = \frac{\partial}{\partial t} + \frac{1}{[1 + (p^n - 1)]!}\frac{\partial^{1+(p^n-1)}}{\partial t} + \cdots = \sum_{k=0}^{\infty} \frac{1}{[1 + k\mu]!}\frac{\partial^{1+k\mu}}{\partial t^{1+k\mu}}$$

to $D_1\varphi'$ and then setting $t = 0$ in the result. This will be proved in the sequel.

5. **Annihilators of modular invariants for $GF[3]$.** First we shall consider the case when the field consists of the classes of residues of integers taken modulo 3. Then (9′) becomes

$$\varphi' - \varphi \equiv t\delta_1\varphi + t^2\delta_2\varphi,$$

where

$$\delta_1 = \Omega + \frac{1}{3!}\Omega^3 + \frac{1}{5!}\Omega^5 + \cdots + \frac{1}{(1 + 2k)!}\Omega^{1+2k} + \cdots$$

and

$$\delta_2 = \frac{1}{2!}\Omega^2 + \frac{1}{4!}\Omega^4 + \frac{1}{6!}\Omega^6 + \cdots + \frac{1}{[2(k + 1)]!}\Omega^{2(k+1)} + \cdots.$$

As indicated in § 4, we are led to suspect that $\delta_2 = \delta_1^2/2!$; at least our hope is enough to warrant our computing $\delta_1^2$. Now

$$\begin{aligned}\delta_1^2 &= \left[\sum_{k=0}^{\infty}\frac{1}{(1 + 2k)!}\Omega^{1+2k}\right]\left[\sum_{l=0}^{\infty}\frac{1}{(1 + 2l)!}\Omega^{1+2l}\right] \\ &= \frac{1}{1!}\Omega^2 + \left[\frac{1}{1!\,3!} + \frac{1}{3!\,1!}\right]\Omega^4 + \left[\frac{1}{1!\,5!} + \frac{1}{3!\,3!} + \frac{1}{3!\,1!}\right]\Omega^6 + \cdots \\ &\qquad + \left[\frac{1}{1!\,(1 + i2)!} + \frac{1}{3!\,[1 + (i - 1)2]!}\right. \\ &\qquad\qquad \left. + \frac{1}{5!\,[1 + (i - 2)2]!} + \cdots\right]\Omega^{2(i+1)} + \cdots.\end{aligned}$$

It is easy to verify for small values of $i$ that the expression inside the braces in each coefficient is identically congruent modulo 3 to $2!$ times the corresponding coefficient in the expression for $\delta_2$ and then proceed by induction. We leave the details to the reader. Thus we have

$$\varphi' - \varphi \equiv t\delta_1\varphi + \frac{t^2}{2!}\delta_1^2\varphi,$$

and it at once follows that a necessary and sufficient condition that $\varphi' \equiv \varphi$ (mod 3) is that $\delta_1\varphi \equiv 0$ (mod 3).

By interchanging $x$ and $y$ and also interchanging $x'$ and $y'$, it follows that a polynomial $\varphi$ in the $a$'s is unaltered under the group of transformations

$$(11)\qquad \begin{aligned} x &= x' \\ y &= tx' + y' \end{aligned} \qquad (t, \text{ any mark in } GF[3]),$$

if and only if

$$(12)\qquad \delta_1' = O + \frac{1}{3!}O^3 + \frac{1}{5!}O^5 + \cdots + \frac{1}{(1+2k)!}O^{1+2k} + \cdots,$$

in which O is the second Aronhold annihilator of the classic theory.

6. **Annihilators of modular invariants for** $GF[p]$. For the set of classes of residues of integers taken modulo a general prime $p$,[*]

$$(13)\qquad \varphi' - \varphi = t\delta_1\varphi + t^2\delta_2\varphi + \cdots + t^{p-1}\delta_{p-1}\varphi,$$

where

$$\delta_k = \sum_{l=0}^{\infty} \frac{1}{[k+l(p-1)]!}\Omega^{k+l(p-1)} \qquad (k = 1, \cdots, p-1).$$

Here

$$\begin{aligned} \delta_1^2 &= \left[\sum_{l=0}^{\infty} \frac{1}{[1+l(p-1)]!}\Omega^{1+l(p-1)}\right]\left[\sum_{r=0}^{\infty} \frac{1}{[1+r(p-1)]!}\Omega^{1+r(p-1)}\right] \\ &= \sum_{s=0}^{\infty}\left[\sum_{q=0}^{s} {}_{2+s(p-1)}C_{1+q(p-1)}\right]\frac{1}{[2+s(p-1)]!}\Omega^{2+s(p-1)}. \end{aligned}$$

Now the expression inside the brackets is congruent to 2 modulo $p$. For, since by Fermat's Theorem

$$(x+y)^{2+s(p-1)} \equiv (x+y)^2 = x^2 + 2xy + y^2 \pmod{p},$$

whenever $x$ and $y$ are integers, the sum of the coefficients of all terms of the form $x^{1+q(p-1)}y^{1+r(p-1)}$ must be congruent to 2 modulo $p$. Thus $\delta_1^2 \equiv 2\delta_2 \pmod{p}$.

Also

$$\begin{aligned} \delta_1^3 &\equiv \delta_1(\delta_1^2) \equiv 2\delta_1\delta_2 \\ &\equiv 2\left[\sum_{l=0}^{\infty} \frac{1}{[1+l(p-1)]!}\Omega^{1+l(p-1)}\right] \times \left[\sum_{r=0}^{\infty} \frac{1}{[2+r(p-1)]!}\Omega^{2+r(p-1)}\right] \end{aligned}$$

---

[*] Dr. Williams reasons thus: "A necessary and sufficient condition that $\varphi'$ be independent of $t$ and so $\equiv \varphi$, modulo $p$, which it is when $t \equiv 0$, modulo $p$, is that $\partial\varphi'/\partial t \equiv \delta_1\varphi$, whence the theorem follows" (Transactions, vol. 22, p. 60). Every part of this statement is self-evident with the exception of the assertion that a sufficient condition that $\varphi' - \varphi \equiv 0 \pmod{p}$ is that $\partial\varphi'/\partial t \equiv 0 \pmod{p}$. Although such a statement is well known to be true when the field of definition is infinite and $\varphi$ is a continuous function of $t$ where $t$ ranges over a continuous interval $(a, b)$, I do not see how one is thereby justified in omitting the proof that the coefficients of the higher powers of $t$ in $\varphi' - \varphi$ are actually the iterations of $\delta_1\varphi$ multiplied by suitable constants, even when the field is finite. It is, however, very easy to give a careful proof.

$$\equiv 2\sum_{s=0}^{\infty}\left[\sum_{q=0}^{s} {}_{3+s(p-1)}C_{1+q(p-1)}\right]\frac{1}{[3+s(p-1)]!}\Omega^{3+s(p-1)}.$$

In this last member, the expression inside the brackets is congruent to 3 (mod $p$), since it is the coefficient of $x^2y$ in $(x+y)^{3+s(p-1)}$ when all exponents are reduced modulo $p-1$. Thus

$$\delta_1^3 \equiv 2\cdot 3\sum_{s=0}^{\infty}\frac{1}{[3+s(p-1)]!}\Omega^{3+s(p-1)} \equiv 3!\,\delta_3.$$

In general, by induction, we have

$$\begin{aligned}
\delta_1^k &\equiv \delta_1(\delta_1^{k-1})\\
&\equiv \left[\sum_{l=0}^{\infty}\frac{1}{[1+l(p-1)]!}\Omega^{1+l(p-1)}\right]\\
&\qquad \times\left[(k-1)!\sum_{r=0}^{\infty}\frac{1}{[(k-1)+r(p-1)]!}\Omega^{(k-1)+r(p-1)}\right]\\
&\equiv (k-1)!\sum_{s=0}^{\infty}\left[\sum_{q=0}^{s} {}_{k+s(p-1)}C_{1+q(p-1)}\right]\\
&\qquad\qquad \times\frac{1}{[k+s(p-1)]!}\Omega^{k+s(p-1)}.
\end{aligned}\tag{15}$$

But the expression inside the last pair of brackets is the sum of the coefficients of all terms of the form

$$x^{(k-1)+(s-q)(p-1)}y^{1+q(p-1)}\tag{16}$$

in the expansion of $(x+y)^{k+s(p-1)}$. But, when $x$ and $y$ are any two integers,

$$(x+y)^{k+s(p-1)} \equiv (x+y)^k = x^k + kx^{k-1}y + \cdots \qquad (\text{mod } p);$$

and thus, since all terms of the form (16) in $(x+y)^{k+s(p-1)}$ coalesce to give the term $x^{k-1}y$ in $(x+y)^k$,

$$\sum_{q=0}^{s} {}_{k+s(p-1)}C_{1+q(p-1)} \equiv k.$$

Therefore (15) gives

$$\delta_1^k \equiv k!\sum_{s=0}^{\infty}\frac{1}{[k+s(p-1)]!}\Omega^{k+s(p-1)} = k!\,\delta_k.\tag{17}$$

Since (17) holds when $k$ has any value from 1 to $p-1$ inclusive, (13) becomes

$$\varphi' - \varphi \equiv t\delta_1\varphi + \frac{t^2}{2!}\delta_1^2\varphi + \cdots + \frac{t^{p-1}}{(p-1)!}\delta_1^{p-1}\varphi.\tag{18}$$

Hence a necessary and sufficient condition that $\varphi' \equiv \varphi$ is that $\delta_1\varphi \equiv 0$ in the field. Thus we have proved

THEOREM I. *Let $S$ be a system of forms in the variables $x$ and $y$ with coefficients, the $a$'s, which may assume any set of values which are integers, reduced modulo $p$, a prime. Let $\varphi$ be a polynomial in the $a$'s. Then a necessary and sufficient condition that $\varphi$ be a modular invariant under the group of transformations $x = x' + ty'$, $y = y'$ is that $\delta_1\varphi \equiv 0$ (mod $p$). Here $\delta_1$ is the differential operator*

$$\Omega + \frac{1}{p!}\Omega^p + \frac{1}{[1 + 2(p-1)]!}\Omega^{1+2(p-1)} + \cdots + \frac{1}{[1 + k(p-1)]!}\Omega^{1+k(p-1)} + \cdots,$$

*in which $\Omega$ is the (first) Aronhold annihilator used in the classic invariant theory. It must be remembered that, since the $a$'s are integers reduced modulo $p$, this theorem requires merely that $\delta_1\varphi$ shall vanish after all possible reductions have been made via Fermat's Theorem.*

7. **A second annihilator for modular invariants in $GF[p]$.** By interchanging the rôles of $x$ and $y$ in the above theorem, we have

THEOREM II. *Let $S$ and $\varphi$ be defined as in Theorem I. Then a necessary and sufficient condition that $\varphi$ be a modular invariant under the group of transformations $x = x'$, $y = tx' + y'$ is that $\delta_1'\varphi \equiv 0$ (mod $p$) where*

$$\delta_1'\varphi \equiv \mathrm{O} + \frac{1}{p!}\mathrm{O}^p + \frac{1}{[1 + 2(p-1)]!}\mathrm{O}^{1+2(p-1)} + \cdots + \frac{1}{[1 + k(p-1)]!}\mathrm{O}^{1+k(p-1)} + \cdots.$$

*Here $\mathrm{O}$ is the second Aronhold annihilator used in the theory of classic invariants and is given by the formula*

$$\mathrm{O}\varphi = \sum_i \frac{\partial\varphi}{\partial a_i}\left(\frac{\partial a_i'}{\partial t}\right)_{t=0}.$$

8. **Two annihilators for formal invariants in $GF[p]$.** In the last three sections, we have been considering modular invariants of $S$ that were not (necessarily) formal and thus the $a$'s were integers reduced modulo $p$. Accordingly, the condition that $\varphi$ be unaltered under the transformation $x = x' + ty'$, $y = y'$ was that $\delta_1\varphi$ shall vanish whenever the $a$'s are in the field. If we now turn our attention to the corresponding problem for formal modular invariants, the $a$'s are no longer integers reduced modulo $p$, but are independent variables and consequently $a^{p^n}$

is no longer congruent to $a$. If we follow through the reasoning of sections 3 to 7, it is evident that the results still hold, provided all the work is purely formal and we do not replace $a^p$ by $a$. Thus we have

THEOREM III. *Let $S$ be a system of forms in the variables $x$ and $y$ with coefficients, the $a$'s, which are independent variables; and let $\varphi$ be a polynomial in the $a$'s. Then a necessary and sufficient condition that $\varphi$ be a formal modular invariant of the system $S$ under the group of transformations $x = x' + ty'$, $y = y'$, where $t$ is any integer reduced modulo $p$, is that $\delta_1\varphi$ be identically congruent to zero, modulo $p$.*

In the same manner, we readily prove the

COROLLARY. *If the coefficients of some forms of the system $S$, say the $a$'s, are independent variables while the coefficients of the other forms of $S$ are integers reduced modulo $p$, then $\varphi$ is a modular invariant of $S$ under the group of transformations $x = x' + ty'$, $y = y'$ (where $t$ is any integer taken modulo $p$) which is formally invariant under the group as to the $\bar{a}$'s if and only if $\delta_1\varphi \equiv 0$, where this congruence is an identity in the $\bar{a}$'s.*

By interchanging the rôles of $x$ and $y$ in Theorem III, we have

THEOREM IV. *Let $S$ and $\varphi$ be defined as in Theorem III. Then a necessary and sufficient condition that $\varphi$ be a formal modular invariant under the group of transformations $x = x'$, $y = tx' + y'$ (where $t$ is any integer reduced modulo $p$) is that $\delta_1'\varphi$ be identically congruent to zero, modulo $p$.*

9. **Two annihilators of modular covariants for $GF[p]$.** By the aid of Theorems III and IV we can readily derive two annihilators of modular covariants (whether formal or otherwise). For it has already been shown that every modular covariant of the system $S(x, y)$—with variables $x$ and $y$—can be obtained in a simple manner from the modular invariants of the system $S'$ consisting of the forms of $S(\xi, \eta)$ and the additional linear $\eta x - \xi y$—in which the variables are $\xi$ and $\eta$.* For every modular covariant of $S(x, y)$ is a polynomial in $L = x^p y - xy^p$ and in the modular invariants $M$ of $S'$ which have been made formally invariant as to $x$ and $y$.

By the Corollary of Theorem III, a function $\varphi$ is a modular invariant of $S'(\xi, \eta)$ under the group of transformations induced by $x = x' + ty'$, $y = y'$ and is formally invariant as to $x$ and $y$ under the group if and only if it is annihilated by

$$\Delta_1 = \Omega' + \frac{1}{p!}\Omega'^{p} + \frac{1}{[1 + 2(p-1)]!}\Omega'^{1+2(p-1)} + \cdots$$

$$= \sum_{k=0}^{\infty} \frac{1}{[1 + k(p-1)]!}\Omega'^{1+k(p-1)},$$

where $\Omega' = \Omega - y\dfrac{\partial}{\partial x}$. Since $L$ is itself a modular invariant of $S'(\xi, \eta)$—

---

* Trans. Amer. Math. Soc., vol. 21 (1920), p. 253.

namely, the invariant which is zero for all classes of $S'(\xi, \eta)$—which has been made formally invariant as to $x$ and $y$, this last statement applies also to $L$ or to any polynomial in $L$ and in the modular invariants $M$ which have been made formally invariant as to $x$ and $y$. Moreover, a necessary and sufficient condition that $\varphi$ be a formal modular covariant of $S$ is that $\Delta_1\varphi$ be identically congruent to zero. Thus we have

THEOREM V. *Let $S$ be a system of forms in the variables $x$ and $y$ with coefficients, the $a$'s, which may assume any set of values which are integers, reduced modulo $p$, a prime. Let $\varphi$ be a polynomial in the $a$'s and in $x$ and $y$. Then a necessary and sufficient condition that $\varphi$ be a modular covariant under the group of transformations $x = x' + ty'$, $y = y'$ (where $t$ is any integer reduced modulo $p$) is that $\Delta_1\varphi \equiv 0 \pmod{p}$. This congruence must be an identity in the variables $x$ and $y$. If, in addition, it is an identity in the $a$'s, then $\varphi$ is a formal modular covariant of $S$.*

If, in Theorem V, we interchange the rôles of $x$ and $y$, we have

THEOREM VI. *Let $S$ and $\varphi$ be defined as in Theorem V. Then a necessary and sufficient condition that $\varphi$ be a modular covariant of $S$ under the group of transformations $x = x'$, $y = tx' + y'$ is that $\Delta_1'\varphi \equiv 0 \pmod{p}$. This congruence must be an identity in $x$ and $y$. When the coefficients of $S$ are independent variables, then $\varphi$ is a formal covariant of $S$ under this group of transformations if and only if $\Delta_1'\varphi \equiv 0 \pmod{p}$, this congruence being an identity in the $a$'s and in the variables $x$ and $y$.*

## Generalization to $GF[p^n]$.

10. **Annihilators for invariants.** Thus far, $t$—the coefficient of the transformation—has been an integer reduced modulo some prime $p$; now we shall generalize and consider the case when $t$ is a polynomial in some variable (say $i$) reduced modulis a polynomial $P(i)$ of degree $n$ and some prime $p$. Thus $t$ is congruent to one of the $p^n$ expressions of the form $c_0i^{n-1} + c_1i^{n-2} + \cdots + c_{n-1}i + c_n$, where the $c$'s range independently over the set of integers $0, 1, \cdots, p - 1$. If $P(i)$ is irreducible modulo $p$, then the set of all such expressions is closed under the processes of addition, subtraction, multiplication and division (provided the divisor is not zero modulis $P(i)$ and $p$), and it is called the Galois Field of order $p^n$—denoted by $GF[p^n]$. For any mark $a$ of this field, we have holding Galois' generalization of Fermat's Theorem, $a^{p^n} \equiv a \pmod{P(i),\ p}$.

Let $S$ be, as before, a system of forms in the variables $x$ and $y$ with coefficients, the $a$'s, which may be independent variables or indeterminate marks of the $GF[p^n]$. A polynomial $\varphi$ in the $a$'s is invariant under the group of transformations

$$\begin{aligned} x &= x' + ty' \qquad (t, \text{ a mark of } GF[p^n]) \\ y &= y' \end{aligned}$$

if and only if the increment of $\varphi$ is congruent to zero in the field. But, by § 3,

$$\varphi' - \varphi = \sum_{k=1}^{\mu} t^k \delta_k \varphi, \qquad (\mu = p^n - 1),$$

where

$$\delta_k \varphi = \sum_{l=0}^{\infty} \frac{1}{[k + l(p^n - 1)]!} \Omega^{k+l(p^n-1)} \qquad (k = 1, \cdots, p^n - 1).$$

This is congruent to zero in the field if and only if each $\delta_k \varphi \equiv 0$.

Now in the work on annihilators for the $GF[p^n]$, we have already shown that

$$\delta_1{}^k \equiv k!\, \delta_k \qquad \pmod{p} \tag{19}$$

when $k = 1, \cdots, p - 1$. These results hold here without change, so that, if $\delta_1 \varphi \equiv 0$, then $\delta_k \varphi \equiv 0$ when $k < p$. But, when $k = p$, although we still have (19) holding, it does not now follow that, if $\delta_1 \varphi \equiv 0$, then so also is $\delta_p \varphi \equiv 0$. For, since $\delta_p \varphi$ is formally congruent to $\delta_1{}^p \varphi / p!$ in the field, then the vanishing of $\delta_p \varphi$ requires that $\delta_1{}^p \varphi \equiv 0$ [mod $pP(i)$ and $p^2$]. Thus, when $n > 1$, there arises a second necessary condition which is independent of the first.

Since the result of dividing by $p + l$—where $l = 1, \cdots, p - 1$—and then reducing modulo $p$ is the same as the result obtained by dividing by $l$ and then reducing modulo $p$, it follows that, when $0 \leqq k < p$,

$$\delta_{k+p} = \frac{\delta_1{}^{k+p}}{(k + p)!} = \frac{\delta_1{}^k}{k!} \frac{(\delta_1{}^p)}{p!} \equiv \frac{\delta_1{}^k}{k!} (\delta_p) \qquad \pmod{p}.$$

Hence, if $\delta_p \varphi \equiv 0$, then $\delta_{k+p} \varphi \equiv 0$ in the field for $0 \leqq k < p$. When $k = p$, we have

$$\begin{aligned} \left[\frac{\delta_1{}^p}{p!}\right]^2 &= \left[\sum_m \frac{1}{[p + m(p^n - 1)]!} \Omega^{p+m(p^n 1)}\right]^2 \\ &= \sum_{m=0}^{\infty} C_m{}^2 \frac{1}{[2p + m(p^n - 1)]!} \frac{\partial^{2p+m(p^n-1)}}{\partial t^{2p+m(p^n-1)}}, \end{aligned}$$

in which

$$C_m{}^2 = \sum_{k=0}^{m} {}_{2p+m(p^n-1)} C_{p+k(p^n-1)}.$$

Now

$$\sum_{k=0}^{m} {}_{2p+m(p^n-1)} C_{p+m(p^n-1)} \equiv {}_{2p}C_p \qquad \pmod{p}$$

since

$$(x + y)^{2p+m(p^n-1)} \equiv (x + y)^{2p},$$

whenever $x$ and $y$ are marks in the field $GF[p^n]$. But ${}_{2p}C_p \equiv {}_2C_1$ modulo $p$, since $\frac{2p-l}{p-l} \equiv 1$ (modulo $p$) when $l \not\equiv 0$ (modulo $p$). Hence

$$\frac{1}{2!}\left[\frac{\delta_1{}^p}{p!}\right]^2 \equiv \delta_{2p} \qquad \text{(mod } p).$$

By induction, we see that

$$\left[\frac{\delta_1{}^p}{p!}\right]^l \equiv (l-1)!\sum_{m=0}^{\infty} C_m{}^l \frac{\partial^{lp+m(p^n-1)}}{\partial t^{lp+m(p^n-1)}} \qquad \text{(mod } p) \tag{20}$$

$$\equiv l!\,\delta_{lp}. \qquad \text{(mod } p).$$

Hence necessary and sufficient conditions that $\delta_k\varphi$ $(k = 1, 2, \cdots, p^2-1)$ shall vanish are that $\delta_1\varphi$ and $\delta_p\varphi$ shall vanish.

More generally, by induction, we see that if $s = k_0 + k_1p + \cdots + k_{n-1}p^{n-1}$ (each $k$ an integer between 0 and $p-1$), then

$$\frac{\delta_1{}^s}{s!} = \frac{1}{(k_0)!}[\delta_1]^{k_0}\frac{1}{(k_1)!}\left[\frac{\delta_1{}^p}{p!}\right]^{k_1}\cdots\frac{1}{(k_{n-1})!}\left[\frac{\delta_1{}^{p^{n-1}}}{(p^{n-1})!}\right]^{k_{n-1}}.$$

Hence we readily prove

THEOREM VII. *Let $S$ be a system of forms in the variables $x$ and $y$ with coefficients, the a's, which may be independent variables or may be indeterminates ranging over the Galois Field $GF[p^n]$ of order $p^n$. Let $\varphi$ be a polynomial in the a's. Then necessary and sufficient conditions that $\varphi$ be an invariant of $S$ under the group of transformations $x = x' + ty'$, $y = y'$ (where $t$ is any mark of $GF[p^n]$) are that $\varphi$ be annihilated in the field by $\delta_k$ where $k = 1, p, p^2, \cdots, p^{n-1}$. Moreover $\varphi$ is a formal invariant of $S$ if and only if these congruences hold identically in the field when the a's are independent variables.*

In a similar manner, we find necessary and sufficient conditions that $\varphi$ shall be an invariant of $S$ under the group of transformations $x = x'$, $y = tx' + y'$ (where $t$ is any mark of the field $GF[p^n]$).

11. **Annihilators for covariants.** We can now readily prove the analogous theorem for covariants, for the modular covariants of a system $S$ are the modular invariants of an enlarged system $S'$. We leave the details of the proof to the reader since they are very similar to those given in § 9. Thus we have

THEOREM VIII. *Let $S$ be a system of forms as in Theorem VII and let $\varphi$ be a polynomial in the a's and in $x$ and $y$. Then necessary and sufficient conditions that $\varphi$ be a covariant of $S$ under the group of transformations $x = x' + ty'$, $y = y'$ (where $t$ is any mark of $GF[p^n]$) are that $\varphi$ be annihilated in the field by $\Delta_k$ where $k = 1, p, p^2, \cdots, p^{n-1}$. Here $\Delta_1$ is defined* *as in* § 9, *and* $\Delta_k = \frac{1}{k!}(\Delta_1)^k$. *Moreover,* $\varphi$ *is a formal covariant of* $S$ *if and only if these congruences* $\Delta_k\varphi \equiv 0$ *hold identically in the field when the* $a$*'s are independent variables.*

In a similar manner, we derive necessary and sufficient conditions that $\varphi$ shall be a covariant of $S$ under the group of transformations $x = x'$, $y = tx' + y'$ (where $t$ is any mark of the field $GF[p^n]$).

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.